DARKTRACE

LIVRE BLANC

Darktrace Antigena: La réponse autonome générée par l'IA

Aperçu général

L'ère actuelle de la cybersécurité est caractérisée par trois défis fondamentaux: la complexité du réseau d'entreprise et de l'infrastructure connectée, la vitesse des attaques récentes et la pression de plus en plus forte exercée sur les intervenants en cas d'incident.

À bien des égards, l'expansion des réseaux et l'adoption continue de nouvelles technologies - des services de cloud à l'Internet des objets (IoT) - ont élargi la surface d'attaque et introduit de nouveaux points d'entrée par lesquels les attaquants peuvent pénétrer. Ceci, combiné à la disponibilité immédiate des kits d'exploits sur le Dark Web, a conduit au « cercle vicieux du Service Operating Center (SOC) », où les intervenants en cas d'incident sont si occupés à réagir aux situations d'urgence qu'ils ont rarement le temps de mettre en œuvre les correctifs critiques qui permettraient de prévenir le problème à sa source.

Alors que les équipes de sécurité ont du mal à faire face au nombre croissant d'attaques de routine, une nouvelle génération de cybermenaces est également apparue, caractérisée en grande partie par des menaces en constante évolution qui ont un impact bien avant que les intervenants humains n'aient le temps de réagir. Ces menaces couvrent des campagnes de ransomware indifférenciées qui se déplacent à la vitesse de la machine, en passant par des vols de données internes et des logiciels malveillants polymorphes qui peuvent se cacher dans le réseau et échapper aux contrôles traditionnels.

En général, les outils de sécurité traditionnels fonctionnent en pré-définissant un comportement « bénin » ou « malveillant » pour identifier et bloquer les menaces connues. Pourtant, cette approche est extrêmement limitée, car elle ne peut détecter de nouvelles menaces, et les nouveaux appareils et systèmes qui composent l'activité numérique sont si complexes et si peu familiers que l'on ne sait pas toujours à quoi ressemblerait un comportement bénin ou malveillant en tout premier lieu.

Lorsque ces outils ont été introduits pour la première fois, l'objectif était de fournir un certain degré d'automatisation pour aider les équipes de sécurité humaine. Cependant, ils se sont révélés insuffisants et parfois contre-productifs, en particulier dans le contexte des actions de blocage perturbatrices et des faux positifs. Compte tenu de ces limitations, une approche plus sophistiquée est nécessaire pour aider les équipes de sécurité déjà très sollicitées à faire face à la complexité numérique et aux menaces en constante évolution telles que les ransomwares.

Grâce aux dernières avancées du Machine Learning (apprentissage automatique) et de l'IA, cette approche a pu être réalisée. La technologie de réponse autonome utilise l'intelligence artificielle pour aider à augmenter la capacité des intervenants humains. Cette technologie basée sur l'intelligence artificielle se caractérise par sa capacité reconnue à contenir les menaces de haute fiabilité en quelques secondes, sans perturber l'activité. Alors que les cybermenaces gagnent en rapidité et en gravité, cette approche est mise à profit pour transformer même les organisations les plus complexes et les plus vulnérables en une entreprise digitale résiliente qui assure sa propre défense.

Avec plus de 7 000 déploiements dans 105 pays à travers le monde, la plate-forme de cyber IA de Darktrace a fourni la première technologie de réponse autonome éprouvée et de qualité professionnelle sur le marché: Darktrace Antigena. Comme un anticorps numérique, la technologie fonctionne en apprenant le « mode de vie » normal de chaque utilisateur et appareil de l'entreprise et en prenant des mesures chirurgicales pour contenir les menaces en cours en temps réel, avant qu'elles n'atteignent le stade de la crise.

Ce livre blanc explore les défis critiques auxquels les équipes de sécurité sont confrontées dans cette nouvelle ère de cybermenace et comment Darktrace Antigena s'appuie sur l'intelligence artificielle pour lutter de manière autonome contre les attaques sophistiquées, donnant ainsi aux équipes de sécurité le temps dont elles ont besoin pour intervenir.

> Darktrace Antigena agit plus rapidement que les autres acteurs de la sécurité pour éviter les conséquences des attaques de type ransomware.
>
> **451 Research**

Stratégies traditionnelles de réponse à un incident

Pour faire face aux menaces émergentes et à la croissance numérique inévitable, les entreprises se sont traditionnellement tournées vers trois stratégies de base pour réagir aux incidents. Bien que ces stratégies aient été viables dans le passé, elles ne sont plus suffisantes et posent souvent de nouveaux défis.

En examinant leurs faiblesses, nous pouvons mieux comprendre pourquoi des milliers d'entreprises adoptent une technologie de réponse autonome basée sur l'IA pour lutter contre les attaques sophistiquées.

Embaucher plus d'intervenants en cas d'incident

Les professionnels qualifiés de la cybersécurité sont au cœur de toute stratégie de cybersécurité mature et au centre du SOC. Cependant, il est devenu évident ces dernières années que la complexité et la vitesse des attaques dépasseront même la meilleure équipe de sécurité. Au moment où les équipes de sécurité ont passé au crible le flot quotidien d'alertes et déterminé que des mesures s'imposaient, il est souvent trop tard pour sauvegarder les données critiques ou protéger suffisamment les éléments essentiels de l'entreprise.

Bien que les responsables de la sécurité ne doivent pas remplacer complètement leurs intervenants en cas d'incident par des machines, l'automatisation sera essentielle pour permettre à leur personnel qualifié de défendre efficacement le réseau, surtout compte tenu de l'ampleur de nos activités et du volume et de la vitesse des attaques entrantes.

Plutôt que de faire appel à davantage d'humains pour gérer la charge de travail croissante, l'objectif de l'entreprise devrait être de minimiser les réactions en situation d'urgence et d'aider les équipes de sécurité à hiérarchiser les activités les plus importantes sur le plan stratégique - de la modernisation des systèmes informatiques à la mise en œuvre des correctifs critiques, en passant par l'assistance aux équipes DevOps et autres sur les nouvelles applications et les déploiements métiers.

Outils d'intervention préprogrammés

Pour compléter les interventions en cas d'incident, les équipes de sécurité ont presque toujours eu recours à une certaine mesure d'automatisation par le biais d'une foule d'outils d'intervention préprogrammés - depuis les pare-feux et les solutions antivirus de la prochaine génération jusqu'aux systèmes de prévention des intrusions et aux passerelles de messagerie sécurisées.

Ces outils sont « préprogrammés » sous deux aspects cruciaux. Tout d'abord, ils s'appuient sur la définition préalable de ce qu'on entend par « bénin » ou « malveillant » en se basant sur la connaissance d'attaques passées et en utilisant généralement des règles, des signatures ou des données de formation. Bien que cette approche puisse bloquer de nombreuses attaques de routine, elle ne parviendra pas à détecter les menaces en constante évolution et les menaces internes subtiles qui peuvent se cacher sous la surface et exfiltrer des données pendant des semaines et des mois. Elle est également connue pour inonder les équipes de sécurité de faux positifs, ce qui alourdit leur charge de travail et les empêche parfois même de réagir aux menaces les plus graves.

D'autre part, ces outils sont « préprogrammés » dans la mesure où leurs actions sont rarement plus sophistiquées qu'un simple blocage ou une mise en quarantaine. Il s'agit essentiellement d'une approche unique qui conduit inévitablement à des actions trop perturbatrices - car même une petite correspondance de signature pourrait faire virer un client du réseau - ou trop fragiles, car les réactions préprogrammées seraient incapables de s'adapter au comportement dynamique d'une attaque polymorphe ou d'une menace interne ingénieuse.

Enfin, ces outils ont généralement une portée assez réduite, car leur domaine de compétence est généralement limité au périmètre, au endpoint ou à la passerelle de messagerie. Cela limite leur capacité à prendre des décisions en temps réel sur la base d'informations corrélées à l'échelle du secteur numérique et à réagir en permanence aux menaces au fur et à mesure de leur développement.

Solutions d'orchestration

Ces dernières années, les équipes de sécurité ont cherché à rationaliser les intégrations et à automatiser les flux de travail en déployant une gamme de solutions d'orchestration, conçues pour mettre en corrélation les informations provenant de différents outils et faciliter la création de playbooks que la machine peut exécuter en votre nom. Bien que ces outils puissent accroître la flexibilité et même offrir la possibilité d'effectuer des nettoyages automatisés - de l'effacement d'ordinateurs portables au remplacement de logiciels et de systèmes d'exploitation - ils présentent des limites et une complexité considérable.

Dans un environnement SOC où les ressources sont limitées et les intervenants débordés, les responsables de la sécurité sont souvent frustrés par les outils d'orchestration qui nécessitent beaucoup d'efforts avant que leurs équipes puissent commencer à tirer profit de cette approche. En particulier, les équipes de sécurité devraient d'abord développer leurs playbooks et comprendre leur fonctionnement ainsi que leurs processus de sécurité avant de pouvoir commencer à écrire les règles que la machine doit mettre en œuvre.

De plus, ces solutions et les nombreux hooks impliqués nécessitent naturellement beaucoup de maintenance et d'entretien pour rester viables. Dans la plupart des cas, il est plus efficace de simplement corriger une vulnérabilité que d'attendre que quelque chose tourne mal et de devoir la contourner.

Plus généralement, même si votre équipe de sécurité a eu du mal à configurer correctement une solution d'orchestration, la technologie est aussi performante que les données qu'elle contient. Cela signifie que ces outils nécessitent non seulement plus de main d'œuvre et d'expertise, mais aussi qu'ils ne parviennent pas à résoudre le problème urgent de l'évolution des menaces qui échappent aux contrôles traditionnels, ni la nécessité de prendre des mesures ciblées plutôt que des mises en quarantaine à grande échelle.

Réponse autonome: La machine contre-attaque

Après avoir fait l'expérience directe de ces limites, les équipes de sécurité les plus avancées optent maintenant pour une approche plus innovante - une approche qui tire parti de la technologie basée sur l'IA pour contenir les menaces en cours à la vitesse de la machine, sans perturber inutilement l'activité.

Cette approche fait ses preuves et repose sur la technologie de réponse autonome - à ne pas confondre avec les premières tentatives d'automatisation – l'une des technologies les plus sophistiquées en matière de cyber IA. D'une manière générale, une solution qui entre dans cette catégorie doit remplir les quatre conditions suivantes :

- Mettre en œuvre des actions ciblées pour contenir les cybermenaces identifiées avec un niveau de confiance élevé
- Ne pas perturber les fonctions de l'entreprise
- Répondre en temps réel
- Lutter contre divers types de menaces, y compris les menaces internes

Mettre en œuvre des actions ciblées pour contenir les cybermenaces identifiées

La technologie de réponse autonome tire parti de l'apprentissage automatique et de l'IA pour laisser de côté le superflu et prendre des mesures chirurgicales basées sur des calculs très fiables du niveau de menace d'une alerte donnée. Bien que ces alertes ne signalent pas toujours les attaques les plus graves, il est désormais évident que l'automatisation dans ce domaine ne peut être efficace que si elle repose sur une approche sophistiquée de la détection des menaces en temps réel. En effet, l'application de l'intelligence artificielle n'est nulle part plus propice qu'à la cybersécurité et ce, par sa capacité à distinguer un ami d' un ennemi même à un niveau granulaire, et à ne faire apparaître que des alertes présentant un risque important. En tirant parti de la cyber IA et en ne neutralisant que les cybermenaces les plus douteuses, la technologie de réponse autonome réduit la charge de travail des analystes et évite les perturbations inutiles de l'activité.

Ne pas perturber les fonctions de l'entreprise

Même si certains outils d'intervention réussissaient à éviter les faux positifs du côté de la détection, le risque de prendre des mesures trop perturbatrices pourrait néanmoins constituer un véritable défi. En effet, la technologie de réponse autonome se distingue non seulement par sa capacité à agir face à des menaces de haut niveau de confiance, mais aussi - et bien plus encore - par sa capacité à prendre des mesures très ciblées et proportionnelles à la menace détectée. Ces mesures sont en capacité de réagir à une situation unique d'une manière qui n'interrompt que les activités potentiellement menaçantes et n'impacte pas le reste des activités.

Répondre en temps réel

Face aux attaques à vitesse machine, le temps est un facteur essentiel et les minutes ou les heures - sans parler des jours - peuvent rapidement entraîner la perte de données précieuses et engendrer d'important coûts monétaires ou réputationnels. Dans le cadre de campagnes de ransomware à propagation automatique, des correctifs peuvent être disponibles dès le début de la champagne. Cependant, les intervenants chargés de défendre des infrastructures vastes et complexes auront du mal à mettre en œuvre ces correctifs du jour au lendemain. Par conséquent, la capacité de la technologie de réponse autonome à agir en quelques secondes est essentielle et explique l'intérêt croissant qu'elle provoque dans cette nouvelle ère de cybermenace.

Lutter contre divers types de menaces

Alors que les outils de réponse traditionnels encouragent généralement une approche cloisonnée et figée de la cyberdéfense, la technologie de réponse autonome est destinée à libérer la puissance de l'entreprise digitale capable de se défendre intégralement. Au fur et à mesure que la surface d'attaque s'étend, le champ d'action de nos technologies de cyberdéfense doit s'étendre avec elle. C'est pourquoi la technologie de réponse autonome couvre les divers environnements numériques et types de menace détectés. Qu'il s'agisse de menaces internes malveillantes ou d'appareils connectés piratés, en passant par les cyber-campagnes lentes et furtives qui passent inaperçues pendant des mois, la technologie de réponse autonome offre une couverture résiliente sur l'ensemble des attaques externes et des menaces internes, et donc sur l'ensemble de l'entreprise digitale.

Se défendre: Darktrace Antigena

Basée sur l'intelligence artificielle primée de Darktrace, Darktrace Antigena représente la première application de technologie de réponse autonome dans l'entreprise. L' approche unique d'auto-apprentissage est pionnière pour la détection des menaces en temps réel, et la plate-forme de cyber IA de Darktrace a évolué pour offrir une automatisation d'une précision chirurgicale qui combat à vitesse machine, en prenant des mesures ciblées pour contenir les menaces en cours avant qu'elles aient le temps de causer des dégâts.

Plutôt que de prédéfinir la menace à l'avance, l'intelligence artificielle de Darktrace analyse les sources de données riches de l'entreprise digitale pour connaître le « mode de vie » de chaque utilisateur, périphérique et toutes les relations entre eux, en utilisant sa compréhension évolutive de la « normalité » pour identifier les déviations subtiles indiquant une attaque en cours.

Lorsque le système détecte une menace de gravité élevée, Darktrace Antigena réagit en quelques secondes - en prenant des mesures proportionnées pour neutraliser la menace et donner à l'équipe de sécurité le temps de répondre. Par exemple, les ransomwares - qui peuvent infecter des dizaines d'ordinateurs en un peu moins de quelques minutes - peuvent être détectés et contenus en 2 secondes environ, évitant ainsi leur propagation au-delà du point de compromis initial.

Tandis que les intervenants humains continuent de pâtir du poids de l'expansion numérique, l'IA de Darktrace prospère face à une complexité croissante. Chaque nouveau point de données apporte plus de détails à la reconnaissance contextuelle d'un comportement « normal », et si des indicateurs disparates d'anomalies apparaissent, ils sont corrélés et contenus avant que la menace ait le temps de se développer. Cela contraste fortement avec la grande majorité des outils de réponse existants, qui ne prennent des décisions qu'en fonction de points de données isolés et dans des délais étonnamment courts.

L'approche probabiliste de Darktrace Antigena est au cœur de sa prétention à l'automatisation précise et ciblée, car elle associe la confiance contextuelle de la détection des anomalies à une réponse mesurée qui ne doit interrompre que ce qui est inhabituel. La gamme d'actions que Darktrace Antigena peut entreprendre s'étend de la reconfiguration des réseaux ou des périmètres à l'interruption des connexions via des réinitialisations TCP, en passant par la modification des autorisations, le gel des comptes et même l'exclusion de périphériques si nécessaire. Dans tous les cas, la compréhension intime du système et des comportements normaux lui permet d'apporter des réponses proportionnées à la menace, qui ne sont ni trop fragiles, ni trop perturbatrices.

Réponse autonome: Dynamique et ciblée

En pratique, il s'agit d'une réponse autonome qui s'adapte à la forme de la menace à mesure qu'elle se développe et devient plus suspecte avec le temps. Supposons, par exemple, que l'IA de Darktrace fasse apparaître un modèle subtil d'activité anormale émanant d'un périphérique du réseau. Dès que le niveau de menace de l'appareil dépasse un seuil minimal, Darktrace Antigena réagit en prenant des mesures granulaires et en bloquant une seule connexion anormale - fermant un canal de commande et de contrôle balisé vers le Portugal.

Cependant, avec le temps, l'implant malveillant a basculé subtilement vers des mécanismes de repli. En s'adaptant au nouveau comportement, l'intelligence artificielle de Darktrace prend en compte l'événement précédent et prend des mesures supplémentaires en réponse, passant de l'interruption d'une connexion unique à l'application du « mode de vie » de groupe de l'appareil, qui ne lui permet d'effectuer que les connexions et transferts de données qu'il ou un groupe de ses pairs effectue habituellement. Au fur et à mesure que la menace s'intensifie, Darktrace Antigena intensifie sa réponse, ne permettant à l'appareil de fonctionner que dans les limites de son mode de vie individuel habituel, et contenant le comportement suffisamment longtemps pour que l'équipe de sécurité puisse enquêter et finalement remédier à la menace.

Ici comme ailleurs, les actions ciblées de Darktrace Antigena ont été ancrées dans une compréhension du comportement normal de l'appareil par rapport à son passé, à son groupe de pairs et à l'ensemble de l'organisation. Alors que l'intelligence artificielle de Darktrace augmente à mesure que la menace se développe, la réaction reste proportionnée dans tous les cas et permet de maintenir le schéma initial de normalité de l'appareil. Tout au long de l'incident, l'utilisateur du périphérique est libre d'utiliser des applications normales et d'accéder aux partages de fichiers habituels, sans même s'apercevoir que l'intelligence artificielle de Darktrace travaille dans les coulisses pour protéger l'entreprise de manière proactive.

> “Darktrace Antigena permet aux organisations de lutter contre les cybermenaces sans perturber les activités quotidiennes.”
>
> **IDC**

Infrastructure digitale capable de s'auto-défendre

Darktrace Antigena répond aux cybermenaces dans l'ensemble du secteur numérique, depuis les réseaux d'entreprise et industriels jusqu'aux conteneurs cloud, aux applications SaaS et même aux communications par email. Cette portée affine non seulement la qualité de la prise de décision de Darktrace Antigena - car elle enrichit la compréhension holistique par le système de ce qu'est un comportement normal et apporte encore plus de contexte à la mesure évolutive de la probabilité de menace - mais elle étend également son champ d'action bien au-delà de la portée limitée des outils de réponse traditionnels.

En effet, alors que la plupart des outils de réponse préprogrammés sont isolés et n'ont donc qu'une seule chance de stopper une attaque émergente (au niveau du périmètre par exemple), l'étendue de Darktrace Antigena couvre toute la chaîne de destruction - que l'attaquant tente de passer du réseau de l'entreprise au cloud, du réseau industriel à l'entreprise ou même d'un dispositif IoT spécifique à un serveur critique.

Grâce à cette protection étendue, Darktrace Antigena est ce qu'il se fait de mieux en matière de réponse autonome – La technologie prend des mesures proportionnées contre les cybermenaces, à vitesse de l'ordinateur et en toute confiance, où que se trouve la menace.

Threat Visualizer et application mobile de Darktrace

L'interface graphique Threat Visualizer de Darktrace fournit une vue unique à partir de laquelle les activités anormales et les actions d'Antigena peuvent être visualisées et analysées en temps réel. Le Threat Visualizer a été conçu pour les utilisateurs de tous les niveaux de maturité, qu'il s'agisse d'experts en sécurité informatique, de responsables métier ou de membres moins expérimentés de l'équipe informatique.

Une multitude d'informations peuvent être triées et affichées de différentes façons en utilisant les fonctionnalités interactives du Threat Visualizer, qui inclut notamment un tableau de bord dynamique où les utilisateurs peuvent filtrer les incidents en fonction de leur niveau de gravité, ainsi qu'un outil interactif Play-Back qui permet de rejouer les incidents et d'évaluer précisément et en temps réel le contexte de chaque événement.

L'application mobile de Darktrace permet également aux utilisateurs d'accéder à ces indications précieuses et de confirmer les actions d'Antigena quand vous êtes à distance. Conçue pour offrir un maximum de flexibilité et augmenter la vitesse d'atténuation, l'application offre des notifications push des attaques en cours et des la possibilitié de confirmer en un clic les réponses suggérées par Antigena. Lorsqu'une attaque survient, les équipes de sécurité peuvent afficher et contenir les menaces en quelques secondes, même lors d'absence du bureau.

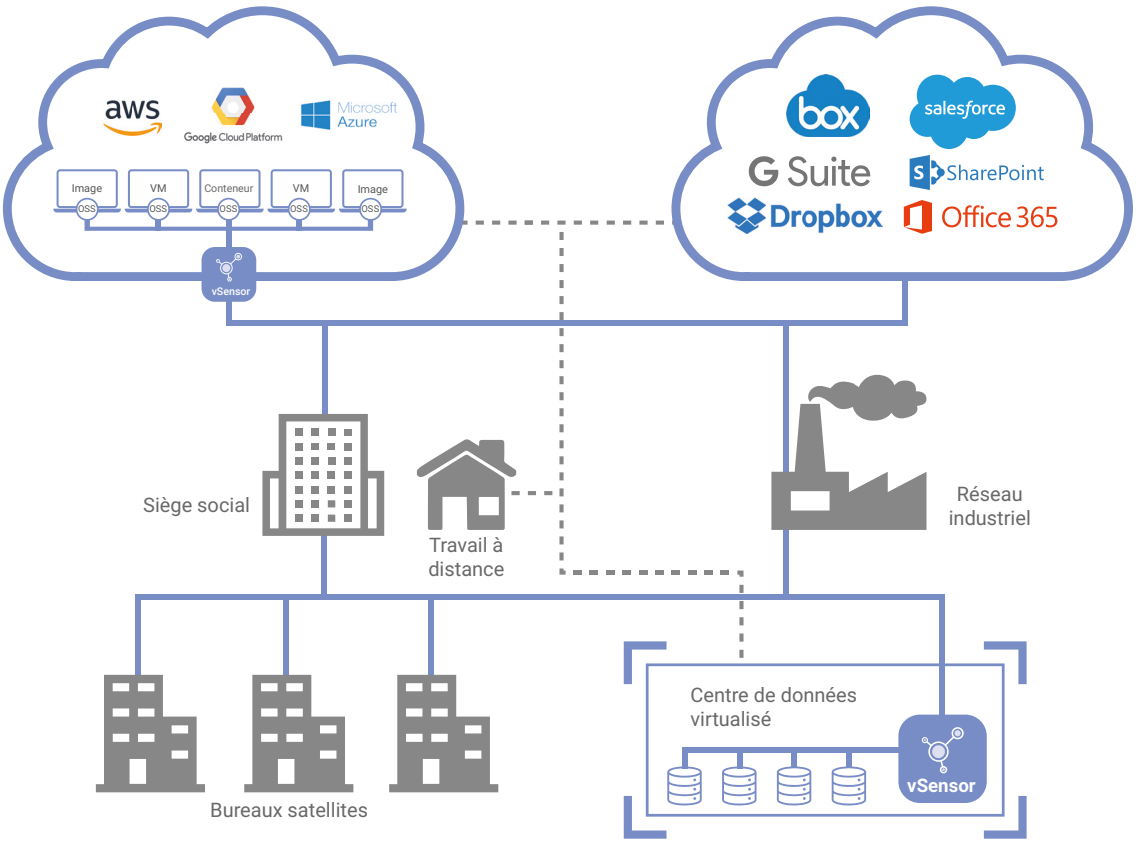

Figure 1: Darktrace Antigena à travers l'infrastructure digitale

Règles d'engagement: Établir la confiance initiale

Darktrace Antigena est entièrement personnalisable et contrôlable; les utilisateurs conservent le contrôle des opérations et peuvent transiter à leur rythme vers une utilisation plus prononcée de l'IA dans leur entreprise.

Pour établir une confiance initiale, les organisations bénéficient invariablement de la possibilité de configurer la portée de Darktrace Antigena en fonction du niveau d'automatisation du système et des cas d'utilisation ciblés, ainsi que des environnements dans lesquels il peut être déployé.

Automatisation configurable

Darktrace Antigena peut être configuré selon l'un des deux modes permettant différents niveaux d'automatisation. Selon le goût du risque de votre entreprise, l'un ou l'autre de ces modes peut être appliqué globalement à l'ensemble de l'organisation ou localement pour un appareil, un système ou un groupe d'utilisateurs donné.

Mode de confirmation humaine

Dans ce mode, Darktrace Antigena génère des réponses qui doivent être validées par l'équipe de sécurité avant que toute action ne soit mise en œuvre. Les clients peuvent approuver facilement les actions proposées par Antigena via l'application Mobile ou le Threat Visualizer de Darktrace. Cela permet aux utilisateurs d'avoir confiance dans la prise de décision d'Antigena avant de passer en mode actif.

Mode actif

En mode actif, Darktrace Antigena est totalement autonome dans les paramètres de fonctionnement définis. Cela signifie qu'une menace peut être instantanément maîtrisée sans qu'un analyste de sécurité ait besoin de se connecter. Les actions lancées en mode actif peuvent également être surveillées via le Threat Visualizer de Darktrace ou l'application mobile.

> "Avec Darktrace, les discussions autour de l'IA en matière de cybersécurité sont devenues des faits concrets."
>
> **Ovum**

Scénarios d'utilisation ciblés

Les organisations peuvent également instaurer la confiance en commençant leurs déploiements par une approche axée sur les cas d'utilisation. Si vous le souhaitez, Darktrace Antigena peut être configuré pour se déclencher sur des catégories de risque spécifiques en fonction du type de menace détecté. Ces catégories incluent les attaques externes, les menaces internes et les risques de conformité, bien que le système puisse également être configuré pour se déclencher sur toute anomalie significative, quel que soit le type de menace.

Attaques externes

Darktrace Antigena peut bloquer la variante de ransomware la plus automatisée, compte tenu de la capacité du système à réagir à la vitesse de l'ordinateur. Dans ce contexte, Darktrace Antigena interrompt généralement les tentatives de chiffrement, les partages internes au réseau ou neutralise les courriers électroniques contenant le ransomware avant qu'ils n'atteignent l'utilisateur. Darktrace Antigena peut également prendre des mesures ciblées sur d'autres formes de logiciels malveillants, en bloquant le téléchargement de fichiers malveillants provenant de sources externes rares ou les tentatives de soustraction aux centres de commande et de contrôle.

Menaces internes

L'intelligence artificielle de Darktrace est également capable de mettre en corrélation de nombreux indicateurs faibles pour identifier les premiers signes d'une menace interne. S'il est configuré pour ce cas d'utilisation, Darktrace Antigena peut agir sur diverses anomalies, allant d'activités utilisateur privilégié inhabituelles aux grands volumes de données sortants, en passant par des téléchargements volumineux inattendus depuis les serveurs internes jusqu'aux machines clientes. Les actions de Darktrace Antigena dans ce contexte pourraient inclure le blocage des connexions SSH et RDP inhabituelles des systèmes non administratifs, ou empêcher les appareils d'envoyer des volumes inhabituellement importants de données vers des appareils externes avec lesquels ils ne communiquent pas normalement.

Conformité

Darktrace Antigena peut également être utilisé pour promouvoir la cyber-hygiène et la conformité, ainsi que pour prévenir les attaques pouvant survenir à l'avenir. Par exemple, Darktrace Antigena peut être configuré pour empêcher de manière sélective les périphériques de communiquer avec des services de partage de fichiers tels que Google Drive, d'empêcher les utilisateurs de se connecter au réseau anonymisant TOR ou d'empêcher l'utilisation du FTP en interne, en externe ou les deux.

Réponse autonome à travers votre infrastructure numérique

Comme l'intelligence artificielle de Darktrace est fondamentalement agnostique à l'égard des divers environnements numériques, les entreprises peuvent également instaurer la confiance en commençant leur déploiement dans des environnements où elles pensent qu'il ajoutera le plus de valeur, puis en étendant sa portée à partir de là.

Domaine de l'entreprise et email

Dans la plupart des déploiements, les entreprises commencent souvent par déployer Darktrace Antigena pour couvrir leurs communications d'entreprise et leurs communications par email, car c'est le système qui ajoutera probablement le plus de valeur dans les domaines de l'entreprise où le volume de travail est le plus important.

La capacité de Darktrace Antigena pour couvrir la messagerie est un atout majeur pour les entreprises qui commencent à peine à mettre en place leurs déploiements de réponse autonome. Darktrace Antigena comble notammment un manque en matière d'outils de sécurité par sa capacité à couvrir à la fois ce qui se passe au niveau de la couche de messagerie externe et ce qui se passe à l'intérieur du réseau. L'IA de Darktrace reconnaît un email malveillant conçu pour provoquer des actions et des activités sur le réseau et peut donc informer les actions autonomes d'Antigena contre des emails similaires ciblant l'entreprise.

> "L'IA de Darktrace détecte les menaces et les arrête immédiatement."
>
> **Penn Highlands Healthcare**

Darktrace Antigena est donc capable de contenir des campagnes d'attaque par courrier électronique contre plusieurs utilisateurs après qu'un seul utilisateur a déjà été infecté sur le réseau. Par exemple, Darktrace peut identifier un email comme étant la source d'activités malveillantes sur le réseau et ainsi permettre à Darktrace Antigena de bloquer des emails similaires ciblant l'entreprise, soit en les supprimant des boîtes de réception de l'entreprise, soit en les empêchant d'atteindre l'utilisateur.

Cette protection préventive peut ainsi arrêter la propagation d'une campagne d'attaque émergente et donnerait aux équipes de sécurité le temps dont elles ont besoin pour intervenir.

Systèmes de contrôle industriels

Compte tenu de la nature critique des environnements industriels en termes de sécurité, Darktrace Antigena est généralement déployé à la frontière des réseaux d'OT, ou entre des réseaux d'entreprise et des réseaux industriels.

Par exemple, les utilisateurs peuvent configurer le système de manière à confiner les sous-traitants à leurs modes de vie individuels lorsqu'ils interagissent avec l'équipement industriel, ou stipuler que les systèmes d'entreprise ne peuvent accéder aux niveaux de stock de la centrale électrique que selon des modalités de routine.

Darktrace Antigena
Menaces Réelles Découvertes

Blocage d'un ransomware sophistiqué

Dans une société internationale de services financiers, une employée a contourné la politique de l'entreprise en vérifiant sa boîte mail personnelle sur un ordinateur portable de l'entreprise. Elle a ouvert ce qu'elle croyait être un document Word, mais était en fait un fichier ZIP malveillant contenant un ransomware. L'appareil a contacté un domaine externe rare et a commencé à télécharger un fichier EXE suspect.

L'intelligence artificielle de Darktrace a identifié cette activité comme extrêmement anormale. Lorsque le fichier exécutable a commencé à chiffrer les partages de fichiers SMB, cela représentait un écart par rapport au 'mode de vie' normal de l'appareil. À ce stade, le système a déterminé que la menace était suffisamment grave pour nécessiter une intervention immédiate.

L'équipe de sécurité n'étant pas sur place pour prendre des mesures face à la situation, Darktrace Antigena a réagi de manière autonome et a interrompu toutes les tentatives d'écriture de fichiers chiffrés sur des partages réseau. Ce faisant, Antigena a neutralisé la menace quelques secondes seulement après le début de l'activité malveillante.

Les attaques de type ransomware comme celles-ci sont de plus en plus courantes et à mesure que de nouvelles souches plus insidieuses apparaissent chaque jour sur le dark web, les ransomwares contournent inévitablement les outils les plus sophistiqués. De plus, les ransomwares sont capables de chiffrer un réseau entier en quelques minutes. Les équipes de sécurité humaine ne peuvent pas faire face à des attaques aussi rapides, et l'autonomie de réaction est devenue vitale dans le contexte actuel de menace.

> "Darktrace Antigena est un multiplicateur de force."
>
> **City of Las Vegas**

Perturbation d'un délit d'initié

Dans une grande chaîne hôtelière en Asie, l'IA de Darktrace a détecté une hausse soudaine de l'activité anormale. Les serveurs externes tentaient d'établir des milliers de connexions à des ordinateurs de bureau distants en devinant les noms d'utilisateur et les mots de passe par défaut.

Darktrace a identifié l'activité comme un écart anormal par rapport au mode de vie du réseau et une enquête plus poussée a révélé que ces tentatives de connexion utilisaient un modèle spécifique, indiquant une attaque automatisée. Darktrace a identifié que certaines de ces connexions de bureau à distance utilisaient des informations d'identification connues.

Le serveur externe était accessible de l'extérieur du réseau avec un compte utilisateur interne. Le serveur a ensuite établi des connexions de bureau à distance entre d'autres ordinateurs de la société avant d'arriver au système de gestion immobilière de l'hôtel, à partir duquel un grand volume de données a été téléchargé.

Un volume comparable de données a tenté de quitter le réseau, en direction du périphérique externe qui avait initié la connexion de bureau à distance d'origine. Ces relations considérées comme très suspectes représentaient un écart extrême par rapport au "mode de vie" normal des appareils.

La direction de l'entreprise a indiqué que le compte utilisateur en question appartenait à un ancien employé qui venait de quitter l'entreprise. Il est possible qu'il ait vendu ses identifiants d'accès avant qu'ils puissent être désactivés, ou qu'il ait tenté de récupérer lui-même les données afin de les vendre à un concurrent.

L'intelligence artificielle de Darktrace a pu détecter et prendre des mesures autonomes en temps réel. Elle a empêché la tentative d'exfiltration de données avant que les informations ne quittent le réseau et a généré un gain de temps précieux pour l'équipe de sécurité.

.

Rapide

Répond en moins de 2 secondes

Ciblé

Arrête les menaces les plus graves

Efficace

10 heures par semaine économisées par analyste de sécurité

Conclusion: L'intelligence artificielle face à la prochaine génération de cybermenaces

La sophistication croissante du paysage actuel de la menace et la complexité grandissante des entreprises numériques ont fait en sorte que des organisations de toutes tailles ont eu du mal à suivre le rythme. Les équipes d'intervention en cas d'incident se retrouvent submergées et sous-financées, et même leurs outils de réponse traditionnels continuent de ne pas être à la hauteur des menaces émergentes. Et pourtant, si ces menaces constituent déjà un défi presque impossible, elles prennent rapidement une nouvelle dimension.

Les cybercriminels ont commencé à tirer parti des avancées de l'IA pour introduire de nouvelles économies d'échelle troublantes dans la lutte. Traditionnellement, les cyber-attaques pouvaient se situer quelque part sur un spectre familier: à une extrémité, il y avait des attaques massives, bien que peu sophistiquées, qui affectaient le paysage mondial, et de l'autre, des attaques avancées et subtiles dirigées contre seulement quelques cibles de grande valeur, car elles étaient toujours limitées par le temps et les effectifs considérables requis pour monter une attaque personnalisée. Avec l'IA, toutefois, les attaquants sont en mesure de développer des outils sophistiqués qui lancent des attaques personnalisées à grande échelle, permettant ainsi aux machines d'analyser rapidement, par exemple, les styles de messagerie et les profils LinkedIn, afin d'envoyer des campagnes de phishing ciblées à des millions de victimes à la vitesse d'une machine.

Alors que les progrès de l'intelligence artificielle continuent d'offrir aux attaquants la possibilité d'améliorer la vitesse, l'échelle et la sophistication des cyber-attaques, la guerre des algorithmes contre les algorithmes est menée au sein des réseaux d'entreprises du monde entier. Les entreprises qui tirent parti de la technologie de réponse autonome basée sur l'intelligence artificielle ont donc une vision claire des choses à venir, car les entreprises d'aujourd'hui doivent être capables de contenir rapidement les attaques, même les plus avancées, avant même d'avoir le temps de sombrer dans une crise.

La technologie d'intelligence artificielle de Darktrace Antigena représente la première technologie de réponse autonome reconnue dans le monde de l'entreprise, et permet aux organisations de se défendre contre cette nouvelle ère de cyber-menace. Darktrace Antigena tire parti de sa compréhension en constante évolution du terme « normal » pour neutraliser les menaces émergentes et arrêter leur propagation en temps réel afin de laisser aux équipes de sécurité le temps d'y répondre.

Avantages clés de Darktrace Antigena

- **Auto-Défense**
  Prend des mesures chirurgicales pour mettre fin aux menaces de gravité élevée
- **Gain de Temps**
  Aide les équipes à hiérarchiser les activités les plus stratégiques
- **En temps réel et 24 heures sur 24**
  Fonctionne en temps réel, 24h / 24 et 7j / 7
- **Personnalisation**
  Configuré en fonction de votre goût pour le risque
- **Flexibilité**
  Contrôlé à distance via l'application mobile Darktrace

> "L'intelligence artificielle de Darktrace est unique et tient réellement ses promesses."
>
> **Forrester**

À propos de Darktrace

Darktrace est leader mondial de l'IA pour la cyberdéfense et le créateur de la technologie de Réponse Autonome. Son IA auto-apprenante reproduit le système immunitaire humain et est utilisée par plus de 3000 organisations afin de se protéger contre les menaces qui pèsent sur les emails, le cloud, l'IoT, ou encore les réseaux bureautiques et industriels.

Darktrace compte plus de 1000 employés et son double siège social est présent à San Francisco et Cambridge, Royaume-Uni. Toutes les 3 secondes, l'IA de Darktrace riposte contre une cybermenace, l'empêchant de provoquer des dégâts.

Contact Us

France : +33 1 40 73 84 85

Canada : +1 41 65 72 20 99

Europe : +44 (0) 12 23 39 41 00

Amérique latine : +55 1 19 72 42 20 11

info@darktrace.com

darktrace.fr